AMENDMENTS TO THE CLAIMS

(IN FORMAT COMPLIANT WITH THE REVISED 37 CFR 1.121)

Please cancel claims 4 and 19 without prejudice.

1. (CURRENTLY AMENDED) A method of transforming between an input signal and an output signal of a circuit, the method comprising the steps of:

(A) copying a plurality of symbols from a source file to a plurality of tables of said circuit;

(B) allocating said input signal among a plurality of block input signals;

(C) generating a plurality of block output signals each responsive to (i) one of said block input signals and (ii) said symbols in one of said tables; and

(D) concatenating said block output signals to form said output signal of said circuit, wherein each of said symbols in said source file has an approximately equal probability of appearance.

2. (PREVIOUSLY PRESENTED) The method according to claim 1, wherein the step of concatenating comprises the sub-steps of:

concatenating said block output signals to form an intermediate result; and

permutating each of a plurality of portions of said intermediate result to present said output signal.

3. (PREVIOUSLY PRESENTED) The method according to claim 1, wherein each of said tables comprise k columns and 2^k rows, where k is a bit width of each of said block input signals and each of said rows stores a unique one of said symbols.

4. (CANCELED)

5. (PREVIOUSLY PRESENTED) The method according to claim 1, further comprising the steps of:

(i) selecting a staring point within said source file to extract said symbols for a first table of said tables;

(ii) calculating a number of symbols extracted for said first table; and

(iii) calculating a subsequent starting point to extract said symbols for a subsequent table of said tables based upon said starting point and said number.

6. (PREVIOUSLY PRESENTED) The method according to claim 5, further comprising the step of:

presenting both a bit width of said block signals and said starting point external to said circuit as a cryptographic key.

7. (PREVIOUSLY PRESENTED) The method according to claim 1, wherein a predetermined number of units of said input signal are allocated to a plurality of said block input signals.

8. (PREVIOUSLY PRESENTED) The method according to claim 7, wherein fewer than said predetermined number of units are allocated to one of said block input signals.

9. (PREVIOUSLY PRESENTED) The method according to claim 1, further comprising the step of:

generating said input signal by counting a clock signal.

10. (PREVIOUSLY PRESENTED) The method according to claim 9, further comprising the steps of:

generating a plurality of said output signals in response to a plurality of said countings; and

concatenating said plurality of output signals to present a second output signal.

11. (CURRENTLY AMENDED) An information recording medium for use in a computer to define a transformation between an input signal and an output signal, the information recording medium recording a computer program that is readable and executable by the computer, the computer program comprising the steps of:

(A) copying a plurality of symbols from a source file to a plurality of tables;

(B) allocating said input signal among a plurality of block input signals;

(C) generating a plurality of block output signals each responsive to (i) one of said block input signals and (ii) said symbols in one of said tables; ~~and~~

(D) concatenating said block output signals to form said output signal; and

(E) generating said input signal by counting a clock signal.

12. (PREVIOUSLY PRESENTED) The information recording medium according to claim 11, wherein the step of concatenating in said computer program comprises the sub-steps of:

concatenating said block output signals to form an intermediate result; and

permutating each of a plurality of portions of said intermediate result to present said output signal.

13. (PREVIOUSLY PRESENTED) The information recording medium according to claim 11, wherein each of said tables comprise k columns and 2^k rows, where k is a bit width of each of said

block input signals and each of said rows stores one of said symbols.

14. (PREVIOUSLY PRESENTED) The information recording medium according to claim 11, wherein each of said symbols in said source file has an approximately equal probability of appearance.

15. (PREVIOUSLY PRESENTED) The information recording medium according to claim 11, wherein said computer program further comprising the steps of:

(i) selecting a staring point within said source file to extract said symbols for a first table of said tables;

(ii) calculating a number of symbols extracted for said first table; and

(iii) calculating a subsequent starting point to extract said symbols for a subsequent table of said tables based upon said starting point and said number.

16. (PREVIOUSLY PRESENTED) The information recording medium according to claim 15, wherein said computer program further comprising the step of:

presenting both a bit width of said block signals and said starting point external to said computer as a cryptographic key.

17. (PREVIOUSLY PRESENTED) The information recording medium according to claim 11, wherein said computer program allocates a predetermined number of units of said input signal to a plurality of said block input signals.

18. (PREVIOUSLY PRESENTED) The information recording medium according to claim 17, wherein said computer program allocates fewer than said predetermined number of units to one of said block input signals.

19. (CANCELED)

20. (CURRENTLY AMENDED) A circuit comprising:

means for copying a plurality of symbols from a source file to a plurality of tables;

means for allocating an input signal among a plurality of block input signals;

means for generating a plurality of block output signals each responsive to (i) one of said block input signals and (ii) said symbols in one of said tables; and

means for concatenating said block output signals to form an output signal, wherein each of said symbols in said source file has an approximately equal probability of appearance.